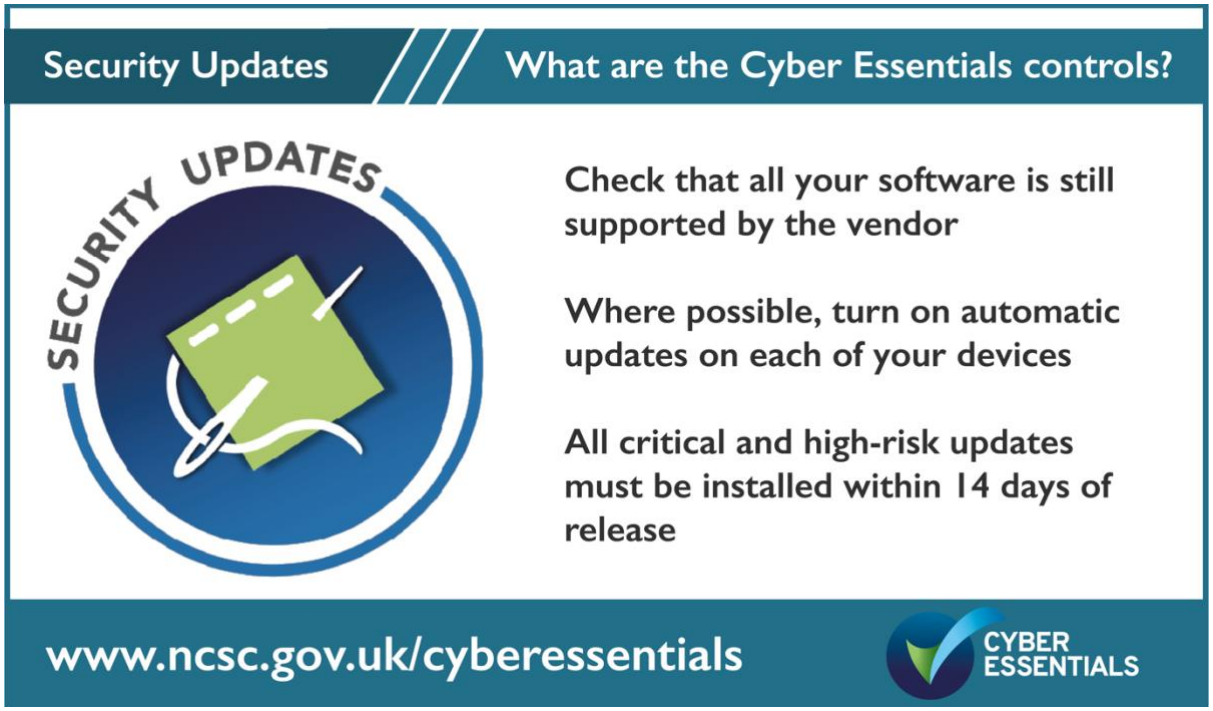

Prevent cyber criminals using the vulnerabilities they find in software as an access point to your systems.

Software and firmware used by your organisation

If hardware is the physical part of a server, computer, tablet or phone, **software** is the set of instructions that 'run' on the device. The operating system, programs and applications are all types of software. **Firmware** is another specific type of software embedded into the hardware of a device to make it function correctly and interact with other software installed on the device. Routers and firewalls contain firmware which acts as the operating system for those devices.

Software and firmware are supported by the manufacturer for a period of time after they have been developed. This support means that if a mistake or weakness, known as a vulnerability, is discovered in the product, the manufacturer will address it with an update or patch which fixes the problem before it can be exploited by cyber criminals.

Knowing which software and firmware you have and whether they are supported is really important. A list of software / firmware is sometimes referred to as a software asset list or inventory. Maintaining an asset inventory helps to track which software you have in use in your organisation. It is important to note that some software requires annual subscriptions to be in place to receive security updates.

Types of software

System software is what is used to manage a computer, an example being the operating system which might be MacOS, WindowsOS or AndroidOS. If a device does not have operating system installed, when switched on, the screen will be blank. System software allows users and hardware to interact with each other.

Application software is any programme that enables the user to complete tasks. Every programme that you use on your device is application software. Examples are Microsoft Word, Excel, internet browsers such as Google Chrome and Apple Safari, and video games. If a device did not have any application software installed, you wouldn't be able to use it for anything other than pre-installed features which come together with an operating system.
Software can be copied from a CD or DVD or downloaded from the internet onto a computer's hard drive/USB drive.
Software as a service (SaaS) is application software that is hosted by a cloud service provider e.g. Microsoft 365 or Dropbox. The software is not downloaded onto the user organisation's IT infrastructure, but accessed remotely from any device and any location.

Firmware is a term for a piece of software that is embedded into the hardware of a device (e.g., a router), in order to make it run properly.

Virtualisation software – A hypervisor is a piece of software that is installed over the hardware of a server to run and manage **virtual machines** on that server.

Patching

Software is made up of thousands of lines of code which is how the computer interprets information to complete its functions. In every 1000 lines of code there is on average 10-15 errors. Most of these errors are not noticeable to you as the user, however, each error is a potential opening for cyber criminals to access your data. These openings are often called 'vulnerabilities'. Within a piece of software's functioning life span, as soon as an error or 'vulnerability' is discovered, the manufacturer creates some additional code to correct the error. This is known as 'patching'. All modern software will need to 'update' on a regular basis (at least every 14 days) as part of its maintenance. This ensures that the latest vulnerabilities that have been discovered are patched within 14 days of the update being made available by the software vendor.

All software must be supported with regular security updates

You should make sure you have ways of keeping each of the following important types of software up to date:
Operating System (OS)
Firmware (in your firewalls and routers)
Web browser and extensions
All applications
Anti-virus

Hypervisors

The easiest and most effective way to ensure that all your software is kept up to date is to turn on automatic updates on each of your devices. This will mean that patches are automatically applied when they are released by the respective vendor. Many devices have automatic updates enabled as default. Some updates might require the device to be manually restarted. If a device hasn't been restarted in a while, then the update might not be installed.

You can check that automatic updates is turned on in settings, under update and security, or systems preferences, under software updates.

For some larger organisations, there is a concern that some software updates may stop other software from working or cause some features to break. Most IT teams in larger organisations aim to fully test each update on a controlled sample of devices, before applying it companywide.

- It is always a good idea to have backups of your data before updating.
- The National Cyber Security Centre has some useful guidance on installing software updates without breaking things

All critical and high-risk updates or updates with no details provided must be installed within 14 days of release by the vendor.

A number of recent high profile cyber attacks have proved that, within a matter of hours, cyber criminals can use a newly discovered software vulnerability to create a mass cyber attack and sent it out to millions of users. Any user that had not installed the patch for that newly found vulnerability would fall victim to that cyber attack. For this reason, it is now a Cyber Essentials requirement that **all** ***high risk and critical updates must be applied within 14 days. Organisations must not be selective about which patches they apply and leave themselves vulnerable.

- Some vendors use different terms to describe the severity of vulnerabilities. 'Critical' or 'high risk' can also be described as a CVSS v3 base score of 7 or

above, which uses the Common Vulnerability Scoring System (CVSS) to provide a numerical representation of the severity of software vulnerabilities.

Unsupported / legacy/ end of life software

When software gets to a certain age, the manufacturer will cease to create and send out patches. The age of software that this occurs varies significantly between vendors. At this point, the software is classed as 'legacy' or 'end of life' as it is no longer supported and therefore no longer secure to use. Not only are the vulnerabilities left un-patched, but they become common knowledge for hackers who create programmes and services to make them easy to exploit, even for criminals with low levels of technical expertise.

Unsupported software should be removed from devices, however, if this isn't possible, it **can** be removed from the certification scope by moving it to a well-defined, segregated and separately managed **sub-set** that prevents all traffic to/from the internet.

The five controls of Cyber Essentials are:

- User Access Control
- **Security Updates**
- Secure Configuration
- Malware Protection
- Firewall and Routers

Help and support

There are over 300 specially trained cyber security companies around the UK who are licensed to certify against the Government's Cyber Essentials Scheme. They can offer help and support in preparation for the assessment. Find one near you.

For questions and feedback about the Cyber Essentials scheme, contact IASME at info@iasme.co.uk or Tel: 03300 882 752